TVET CERTIFICATE V in NETWORKING

DATA BACK UP AND RECOVERY

NEWBR501

Perform data backup and recovery

Competence

Learning hours: 60

Credits: 6

Sector: ICT

Sub-sector: NEWORKING

Module Note Issue date: June, 2020

Purpose statement

This module is intended to the learner pursuing TVET certificate V in networking, at the end of this module the learner will be able to write an IT disaster recovery Plan, Implement the written IT disaster Recovery, Document the work done, and he or she will be able to work competitively in the ICT world under non directive supervision.

Table of Contents

<u>Total Number of Pages:</u> 34

Learning Unit 1 – Write an IT disaster recovery Plan

LO 1.1 – Identify and Analyze Disaster Risks/Threats

- Content/Topic 1: Classification of Risks Based on Relative Weights

A. Definition of risk.

Risk is the possibility of something bad happening. Risk involves uncertainty about the effects/implications of an activity with respect to something that humans value (such as health, well-being, wealth, property or the environment), often focusing on negative, undesirable consequences. Many different definitions have been proposed. The international standard definition of risk for common understanding in different applications is "effect of uncertainty on objectives". The understanding of risk, the common methods of analysis and assessment, the measurements of risk and even the definition of risk differ in different practice areas (business, economics, environment, finance, information technology, health, insurance, safety, security etc).

B. Classification of Disaster risks

1. External Risks

External risks are those that cannot be associated with a failure within the enterprise. They are very significant in that they are not directly under the control of the organization that faces the damages.

External risks can be split into four subcategories:

- **Natural:** These disasters are on top of the list in every disaster recovery plan. Typically, they damage a large geographical area.
- **Human caused**: These disasters include acts of terrorism, sabotage, virus attacks, operations mistakes, crimes, and so on. These also include the risks resulting from manmade structures. These may be caused by both internal and external persons.
- **Civil**: These risks typically are related to the location of the business facilities. Typical civil risk includes labor disputes ending in strikes, communal riots, local political instability, and so on. These again may be internal to the company or external.
- **Supplier**: These risks are tied to the capacity of suppliers to maintain their level of services in a disaster. It is appropriate that a backup supplier pool be maintained in case of emergency.

2. Facility Risks

Facility risks are risks that affect only local facilities. While evaluating these risks, the following essential utilities and commodities need to be considered.

- **Electricity:** To analyze the power outage risk, it is important to study the frequency of power outage and the duration of each outage. It is also useful to determine how many powers feeds operate within the facility and if necessary make the power system redundant.
- **Telephones**: Telephones are a particularly crucial service during a disaster. A key factor in evaluating risks associated with telephone systems is to study the telephone architecture and determine if any additional infrastructure is required to mitigate the risk of losing the entire telecommunication service during a disaster.
- **Water**: There are certain disaster scenarios where water outages must be considered very seriously, for instance the impact of a water cut off on computer cooling systems. Climate Control: Losing the air conditioning or heating system may produce different risks that change with the seasons.
- **Fire**: Many factors affect the risk of fire, for instance the facility's location, its materials, neigh boring businesses and structures, and its distance from fire stations. All of these and more must be considered during risk evaluation.

3. Data Systems Risks

Data systems risks are related to the use of shared infrastructure, such as networks, file servers, and software applications that could impact multiple departments. A key objective in analyzing these risks is to identify all single points of failure within the data systems architecture.

Data systems risks can also be due to inappropriate operation processes. Operations that have run for a long period of time on obsolete hardware or software are a major risk given the lack of spares or support. Recovery from this type of failure may be lengthy and expensive due to the need to replace or update software and equipment and retrain personnel.

Data systems risks may be evaluated within the following subcategories:

- Data communication network
- Telecommunication systems and network
- Shared servers
- Virus
- Data backup/storage systems
- Software applications and bugs

4. Departmental Risks

Departmental risks are the failures within specific departments. These would be events such as a fire within an area where flammable liquids are stored, or a missing door key preventing a specific operation.

An effective departmental risk assessment needs to consider all the critical functions within that department, key operating equipment, and vital records whose absence or loss will compromise operations. Unavailability of skilled personnel also can be a risk. The department should have necessary plans to have skilled backup personnel in place.

5. Desk-Level Risks

Desk-level risks are all the risks that can happen while limiting or stopping the day-to-day personal work of an individual employee. The assessment at this layer may feel a little like an exercise in paranoia. Every process and tool that makes up the personal job must be examined carefully and accounted as essential.

Content/topic 2: Building the Risk Assessment.

Once the evaluation of the major risk categories is completed, it is time to score and sort all of them, category by category, in terms of their likelihood and impact. The scoring process can be approached by preparing a score sheet that has the following keys:

- **Groups** are the subcategories of the main risk category.
- **Risks** are the individual risks under each group that can affect the business.
- **Likelihood** is estimated on a scale from 0 to 10, with 0 being not probable and 10 highly probable. The likelihood that something happens should be considered in a long plan period, such as 5 years.
- **Impact** is estimated on a scale from 0 to 10, with 0 being no impact and 10 being an impact that threatens the company's existence. Impact is highly sensitive to time of day and day of the week.
- **Restoration Time** is estimated on a scale from 1 to 10. A higher value would mean longer Restoration time hence the priority of having a Disaster Recovery mechanism for this risk is Higher.

Content/topic 3: Determining the Effects of Disasters.

A. Disasters

Disasters are inevitable but mostly unpredictable, and they vary in type and magnitude.

The best strategy is to have some kinds of disaster recovery plan in place, to return to normal after the disaster has struck.

For an enterprise, a disaster means abrupt disruption of all or part of its business operations, which may directly result in revenue loss.

To minimize disaster losses, it is very important to have a good disaster recovery plan for every business subsystem and operation within an enterprise.

Disasters are sudden calamitous event bringing great damage, loss, or destruction

The first step in planning recovery from unexpected disasters is to identify the threats or risks that can bring about disasters by doing risk analysis covering threats to business continuity.

Risk analysis (sometimes called business impact analysis) involves **evaluating** existing physical and environmental security and control systems, and **assessing** their adequacy with respect to the potential threats.

Once the disaster risks have been assessed and the decision has been made to cover the most Critical risks, the next step is to determine and list the likely effects of each of the disasters. These Specific effects are what will need to be covered by the disaster recovery process.

B. List of Disaster Affected Entities

The intention of this exercise is producing a list of entities affected by failure due to disasters, which need to be addressed by the disaster recovery plan. The entities that fail due to the earthquake disaster are office facility, power system, operations staff, data systems, and telephone system.

The following table provides a sample mapping of the cause, effects, and affected entities.

Risk (Disaster)	Effect of Disaster	Disaster affected Entity
Earthquake	Office space destroyed	Office space
	Operators cannot report to work	Office staff
	Power disruption	Power
	Data systems destroyed	Data systems
	Desktops destroyed	Desktops and workstations
	Telecom failure	Telephone instruments and network
Power supply cut	Power disruption	Power
	Data systems powered off	Data systems
	Desktops powered off	Desktops/workstations
	Data network down	Network devices and links
	Telecom failure	Telephone instruments and network

C. Downtime Tolerance Limits

Once the list of entities that possibly fail due to various types of disasters is prepared, the next step is to determine what the downtime tolerance limit is for each of the entities. This information becomes crucial for preparing the recovery sequence in the disaster recovery plan.

The entities with less downtime tolerance limit should be assigned higher priorities for recovery. One metric for evaluating the downtime tolerance limit is the cost of downtime.

D. Cost of Downtime

The cost of downtime is the main key to calculate the investment needed in a disaster recovery plan. Downtime costs can be divided into tangible and intangible costs. Tangible costs are those costs that are a consequence of a business interruption, generating loss of revenue and productivity.

Intangible costs include lost opportunities when customers would approach competitors, loss of Reputation, and similar factors.

E. Interdependencies

How the disaster affects entities depending upon each other, is crucial information for preparing the recovery sequence in the disaster recovery plan. For example, having the data systems restored has a dependency on the restoration of power.

- Content/topic 3: Evaluation of Disaster Recovery Techniques.

Data should be replicated on a secondary site **to assure a greater availability and security of systems and business continuity**. The secondary site will become operational when the primary site is unavailable for any reason.

A. Synchronous replication

When data and systems are replicated on both the secondary site and locally, the replication is named synchronous. This kind of technique guarantees the business continuity and a fast restore of processes. It is the best solution to minimize downtimes and assure a high infrastructural availability.

Most synchronous replication products write data to primary storage and the replica simultaneously. As such, the primary copy and the replica should always remain synchronized.

The synchronous replication has a geographic limit: the two sites cannot be far away from each other more than 100 kilometers, otherwise the synchronous couple become less effective and performances decreased.

B. Asynchronous replication

In contrast, asynchronous replication products copy the data to the replica after the data is already written to the primary storage. Although the replication process may occur in near real time, it is more common for replication to occur on a scheduled basis. For instance, write operations may be transmitted to the replica in batches on a periodic basis (for example, every one minute). In case of a fail-over event, some data loss may occur.

C. Mixed techniques

It enables to minimize recovery times, and at the same time, ensures the availability of services even with expanded disasters. It consists of replicating systems with the synchronous technique on a relatively close site and makes a second replication on a distant place.

D. Disaster Recovery Committee

Disaster recovery operations and procedures should be governed by a central committee. This committee should have representation from all the different company agencies with a role in the disaster recovery process, typically management, finance, IT (multiple technology leads), electrical department, security department, human resources, vendor management, and so on.

The Disaster Recovery Committee creates the disaster recovery plan and maintains it. During a disaster, this committee ensures that there is proper coordination between different agencies and that the recovery processes are executed successfully and in proper sequence.

The Disaster Recovery Committee should be authorized and responsible for:

- Creating and maintaining the disaster recovery plan
- Detecting and announcing disaster events within the company
- Activating the disaster recovery plan
- Executing the disaster recovery plan

- Monitoring the disaster situation continuously and returning operations to normal at the earliest feasible time
- Restoring normal operations and shutting down disaster recovery operations
- Continuously improving the disaster recovery plan by conducting periodic mock trials and incorporating lessons learned into the plan after an actual disaster

Notice: Not all the members of the Disaster Recovery Committee may actively participate in the actual disaster recovery. But, several key members of the committee, such as the operations manager, operations coordinator, and the respective operations team leads, will always actively participate.

LO1.2 - Describe disaster recovery phases

- Content/Topic 1: Preparation for Back up

A **backup** or **data backup** is a copy of **computer data** taken and stored elsewhere so that it may be used to restore the original after a **data loss** event.

Backups can be used to recover data after its loss from data deletion or corruption, or to recover data from an earlier time.

Backups provide a simple form of disaster recovery; however not all backup systems are able to reconstitute a computer system or other complex configuration such as a computer cluster, active directory server, or database server.

A backup system contains at least one copy of all data considered worth saving. The data storage requirements can be large. An information repository model may be used to provide structure to this storage.

1. **Types of backup**

a. **Full backups**

A full backup is exactly what the name implies; It is a full copy of your entire data set.

Although full backups arguably provide the best protection, most organizations only use them on a periodic basis because they are time-consuming and often require a lot of disk or tape capacity.

Because not every organization has the time or storage space for frequent full backups, other types are often necessary.

b. **Incremental backups**

Incremental backups only back up the data that has changed since the previous backup.

For example, suppose that you created a full back up on Monday and used incremental backups for the rest of the week. Tuesday's scheduled backup would only contain the data that has changed since Monday. Wednesday's backup would only contain the data that has changed since Tuesday, and so on.

Incremental backups were introduced as a way to decrease the amount of time and storage space that it takes to do a full backup.

c. Differential backups

A differential backup is similar to an incremental backup in that it starts with a full backup and subsequent backups only contain data that has changed. The difference is that while an incremental backup only includes the data that has changed since the previous backup, a differential backup contains all of the data that has changed since the last full backup.

d. Local back-up

Local backup is probably familiar to many. It simply refers to back up that is stored at close proximity. In most cases of local backup, the storage device is connected directly to the source or through a network.

e. Offsite backup

Provided that the backup is stored in a geographically separate location, the type of backup is offsite. And yes, the backup may be done locally and stored in an external hard disk.

If the storage medium is taken to a different location, then it is an offsite backup. It could mean that you have taken the drive home, to your safe deposit box and to another building.

f. Cloud backup

The location of cloud backup is online servers. It is one of the most effective and preferred types of backup. Cloud backup can be accessed from anywhere even in the most remote of places. All that you will be expected to have are login credentials.

g. File Transfer Protocol (FTP) backup

What is basically means is that the backup operation is done through a file transfer protocol and the data is stored in an FTP server through the internet. Where is an FTP server located? It is found in a commercial data center.

h. Mirror Backup

Mirror backups are as the name suggests a mirror of the source being backed up. With mirror backups, when a file in the source is deleted, that file is eventually also deleted in the mirror backup. Because of this, mirror backups should be used with caution as a file that is deleted by accident or through a virus may also cause the mirror backups to be deleted as well.

i. Full PC Backup or Full Computer Backup

In this backup, it is not the individual files that are backed up but entire images of the hard drives of the computer that is backed up. With the full PC backup, you can restore the computer hard drives to its exact state when the backup was done. With the Full PC backup, not only can the work documents, picture, videos and audio files be restored but the operating system, hard ware drivers, system files, registry, programs, emails etc. can also be restored.

j. Online Backup

These are backups that are ongoing or done continuously or frequently to a storage medium that is always connected to the source being backed up. Typically, the storage medium is located offsite and connected to the backup source by a network or Internet connection. It does not involve human intervention to plug in drives and storage media for backups to run. Many commercial data centers now offer this as a subscription service to consumers. The storage data canters are located away from the source being backed up and the data is sent from the source to the storage data center securely over the Internet.

k. Remote Backup

Remote backups are a form of offsite backup with a difference being that you can access, restore or administer the backups while located at your source location or other location. You do not need to be physically present at the backup storage facility to access the backups. For example, putting your backup hard drive at your bank safe deposit box would not be considered a remote backup. You cannot administer it without making a trip to the bank. Online backups are usually considered remote backups as well.

1. Data Recovery

In computing, **data recovery** is a process of salvaging (retrieving) inaccessible, lost, corrupted, damaged or formatted data from secondary storage, removable media or files, when the data stored in them cannot be accessed in a normal way. The data is most often salvaged from storage media such as internal or external hard disk drives (HDDs), solid-state drives (SSDs), USB flash drives, magnetic tapes, CDs, DVDs, RAID subsystems, and other electronic devices. Recovery may be required due to physical damage to the storage devices or logical damage to the file system that prevents it from being mounted by the host operating system (OS).

2. Disasters

Disaster can be the result of three broad categories of threats and hazards. The first category is natural hazards that include acts of nature such as floods, hurricanes, tornadoes, earthquakes, and epidemics. The second category is technological hazards that include accidents or the failures of systems and structures such as pipeline explosions, transportation accidents, utility disruptions, dam failures, and accidental hazardous material releases. The third category is human-caused threats that include intentional acts such as active assailant attacks, chemical or biological attacks, cyberattacks against data or infrastructure, and sabotage. Preparedness measures for all categories and types of disasters fall into the five mission areas of prevention, protection, mitigation, response, and recovery.

3. Disaster recovery

Disaster Recovery involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems supporting critical business functions.

As opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events? Disaster recovery can therefore be considered a subset of business continuity.

- *Recovery Time Objective (RTO):* is the time that it takes to recover data and applications, meaning, how long it will be until business operations are back to normal after an outage or interruption.
- *Recovery Point Objective (RPO):* is the last point-in-time IT systems and applications can be recovered to. It indicates the amount of data that will be lost, measured in elapsed time.

4. Disaster recovery plan:

Includes processes, policies and procedures that are necessary for the recovery of operations and the continuations of the critical functions of an organization after a disaster.

Importance of disaster recovery plan

It is important because:

- It returns the organization to normal operations
- Limits the effect of the disaster onto the organization
- Minimize the occurrence of certain types of disaster in the future

5. Backup devices and media

In computer technologies, a backup storage device is used to make copies of data that is actively in use.

Backup machines provide redundancy of data residing on primary storage.

Storage medium, such as a **hard disk drive (HDD)**, fail or become corrupted, the original data is recovered from copies on the backup hardware. The use of backup storage is imperative in enterprise environments, in which the loss of business data is potentially catastrophic.

There's a bewildering variety of things you can back up onto.

- Floppy disks
- Magneto optical and disks floptical disks
- Optical disks
- Hard drives and disks
- Magnetic tapes
- Jukeboxes, stack loaders, etc.

✓ Floppy disks

On PCs, diskettes are often used for backups. Their low storage capacity makes this an impractical means of doing a full backup on a Unix workstation. However, this method is better than nothing and can be used in a pinch for individual files or directories. They are inexpensive and can be fairly reliable if stored correctly.

1. How should floppy disks be stored?

- Laying flat.
- Sitting upright.

✓ Magneto optical and floptical disks

Magneto optical disks are the same length and width as a 5 1/4 inch floppy disk, but thicker. They can store 128MB-1.2GB of raw data. They can be more stable than magnetic media, such as tapes, because they are written magnetically and read optically. This means that reading does not degrade the stored data. The drives are quite expensive as are the disks themselves.

Floptical disks utilize the same technology as magneto optical disks. They have a smaller storage capacity of 21-120MB of raw data. Most floptical drives can read and write to basic floppy diskettes.

✓ **Optical disks**

Optical disks have a storage capacity from 128MB to 2GB on a 4.6-inch compact disk. They use a laser for writing and reading to the disk. They offer high capacity storage but are 2 to 3 times slower than hard drives. There are three primary types used for storage:

CD-ROM (compact disk - read only memory)

> CD-ROM is the most common optical disk type, and is used by the music industry as well. This is not useful for backups but is a good choice for archiving large pools of static data.

WORM (write once read many)

A write-once CD-ROM drive is another viable, although expensive, backup option. Recordable CDs are usually less expensive than optical disks. Once written, the data is permanently recorded. Current raw storage capacities are from 540 to 640 MB.

Rewritable optical disks

Rewritable optical disks typically are commonly used for data backup and archiving data. The drives and disk are generally fairly costly but both fast and reliable.

- ✓ **Hard drives and disks**

A hard drive can also be used to create a disk image backup, where all the data on one hard disk is simply copied to another hard disk. The second disk can be used as a backup if the first drive should fail. With the recent reduction in the cost of hard drives this option is more attractive. However, there are a couple problems with this method. For example, since it is difficult to store (multiple) disk drives off-site, this would not be a good backup method in a disaster-recovery situation. Previous versions of the same file would be unavailable.

- ✓ **Magnetic tapes**

Magnetic tape is the most realistic medium for creating Unix backups. The tape is actually a mylar film strip on which information is stored. It is the traditional backup medium that has been in use for years. Magnetic tapes are a sequential storage device. Since tape drives cannot randomly access data like other storage devices, such as disk drives, they are much slower. However, high storage capabilities and low cost make magnetic tapes the storage medium of choice for archiving large amounts of data.

9-track tape (also called half-inch tape) is the old standard in magnetic tape storage. It consists of half-inch tape wound on a circular reel. Although these tapes are still in use, they are extremely bulky and the storage capacity is small by today's standards. A 9-track tape will only hold around 225MB at the highest density.

QIC (quarter inch cartridge) tapes are reliable and were widely used several years ago. The drives are inexpensive, but slow. Current storage capacity of QIC tapes is up to 2GB, however, more common capacities are 150MB, 320MB, and 525MB.

DAT (digital audio tape) or helical scan devices come in two standard sizes, 8mm and 4mm. 4mm DAT's support storage capacities from 1-8 GB, while 8mm DAT's support storage capacities from 2-10 GB. 8mm and 4mm tapes are most common on newer systems. 4mm tapes are physically the smallest of the magnetic tapes and therefore take up less storage room. The only disadvantage of these tapes seems to be that they are more sensitive to heat damage than other types of tape. 8mm and 4mm tapes come in two grades; one for video/audio recording and one for binary data. The video/audio tapes may work for making backups, but they are less reliable in terms of retaining data. The binary grade tapes are a better choice. The 4mm is currently the most widely used but is being replaced by DLT.

DLT (digital linear tapes) have a storage capacity of up to 40GB with compression. The drives are quite fast and are the newest standard backup media technology. For recommended reading on the Quantum Corporation's DLT technology, see, DLT Technology -- Delivering Data Protection You Can Depend On and DLT Frequently Asked Questions.

2. Which type of magnetic tape is the best choice for unattended backups?

- DLT tapes are best.
- DAT tapes are best.
- It depends on how much space the backup will take.

- ✓ **Jukeboxes, Stack loaders, etc**

Jukeboxes and stack loaders are designed to automate the handling of media to single or multiple DAT, DLT, or optical drives. They are also known as tape or optical libraries. These devices are able to load and unload tapes into removable media drives on an as needed basis.

- Content/Topic 2: Description of Three Disaster Recovery phases.

Phase 1: Activation Phase

A disruption or emergency may happen with or without notice. Quick and precise detection of a disaster event and having an appropriate communication plan are the keys for reducing the effects of the incoming emergency; in some cases, it may give enough time to allow system personnel to implement actions gracefully, thus reducing the impact of the disaster.

In this phase, the disaster effects are assessed and announced.

1. **Notification Procedures**

The notification procedure defines the primary measures taken as soon as a disruption or emergency has been detected or definitely predicted. At the end of this phase, recovery staff will be ready to execute contingency actions to restore system functions on a temporary basis.

Procedures should contain the process to alert recovery personnel during business and non-business hours. After the disaster detection, a notification should be sent to the damage assessment team, so that they can assess the real damage occurred and implement subsequent actions.

Notification information may contain the following

- ✓ Nature of the emergency that has occurred or is imminent
- ✓ Loss of life or injuries
- ✓ Damage estimates
- ✓ Response and recovery details
- ✓ Where and when to assemble for briefing or further response instructions
- ✓ Instructions to prepare for relocation for estimated time period.

2. **Damage Assessment**

To establish how the contingency plan will be executed following a service disruption, it is crucial to evaluate the nature and degree of the damage to the system. This damage evaluation should be done as quickly as conditions permit, with personnel safety given highest priority. Consequently, when possible, the damage assessment team is the first team notified of the incident.

It is worthwhile to prepare damage assessment guidelines for investigating different types of major alarms that may progress to a disaster. An example might be a sudden power outage noticed in a data center facility that has a UPS backup.

The investigation may determine whether the power can be restored before the UPS system runs out of battery power, in which case activating the disaster recovery plan is not necessary, or otherwise, in which case the plan may be activated immediately.

Damage assessment procedures vary with each particular emergency; nevertheless, the following may be considered in general:

- Origin of the emergency or disruption
- Potential for additional disruptions or damage
- Area affected by the emergency
- Status of physical infrastructure
- Inventory and functional status of the most important equipment
- Type of damage to equipment
- Items to be replaced
- Estimated time to restore normal services if disaster procedures were not in place

3. Activation Planning

While it is beneficial to detect a disaster at its earliest stage, putting a disaster recovery process into action for a false alarm may stall normal business operations and result in undue costs. Hence it is very important that disaster recovery be activated only when a thorough damage assessment has been conducted.

The disaster recovery plan should have one or more criteria for activation, which become the primary input for evaluating whether the plan should be activated for each affected system. Also, it should be determined whether activating disaster response will bring systems back on line faster than standard procedures.

Depending on the extent of the damage from the disaster, the entire Disaster Recovery Committee or a part of the committee may do the disaster activation planning.

The outcome of this planning, at a minimum, should be:

- List of systems and services that need to be restored
- Their interdependencies and sequence of restoration
- Time estimations for each restoration (documented in the plan)
- Instructions for reporting failures to the team leads
- Plan for communication between teams

Once the disaster activation is planned, the appropriate team leads will notify staff and start their respective activities in sequence as they have been instructed.

Phase 2: Execution Phase

Recovery operations start just after the disaster recovery plan has been activated, appropriate operational staff has been notified, and appropriate teams have been mobilized. The activities of this phase focus on bringing up the disaster recovery system. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site.

In this phase, the actual procedures to recover each of the disaster affected entities are executed. Business operations are restored on the recovery system.

1. **Sequence of backup activities**

Daily tasks are the operational fundamentals that most backup administrators are familiar with and include items such as:

- Job monitoring
- Success/failure reporting
- Problem analysis and resolution
- Tape handling and library management
- Scheduling

Weekly, monthly and long-term activities focus on:

- Performance analysis
- Capacity trending and planning
- Policy review and analysis

- Recovery testing and verification

- Architecture planning and validation

2. Sequence of Recovery Activities

The recovery procedure reflects priorities previously analyzed during the activation-planning phase. For instance, if a server room has been recovered after a disruption, the most critical servers should be restored before other, less critical servers.

The procedures should also include instructions to coordinate with other teams when certain situations occur, such as:

- An action is not accomplished within the estimated time frame
- A key step has been completed
- Items must be procured

If a system must be recovered at a different location, specific items related to that service need to be transferred or obtained. Recovery procedures should delegate a team to manage shipment of equipment, data, and vital records. Procedures should explain requirements to package, transport, and purchase materials required to recover the system.

3. Recovery Procedures

The disaster recovery plan should provide detailed procedures to restore the system or system components. Procedures for IT service damage should address specific actions such as:

- Get authorization to access damaged premises or geographic area
- Notify users associated with the system
- Obtain required office supplies and work space
- Obtain and install required hardware components
- Obtain and load backup media
- Restore critical operating systems and application software
- Restore system data
- Test system functionality including security controls
- Connect system to network or other external systems

To avoid confusion in an emergency situation, the recovery procedures should be documented in a simple step-by-step format, without assuming or omitting any procedural steps.

Phase 3: Reconstitution phase

In the reconstitution phase, operations are transferred back to the original facility once it is free from the disaster after effects, and execution-phase activities are subsequently shut down. If the original system or facility is unrecoverable, this phase also involves rebuilding.

Hence the reconstitution phase may last for a few days to few weeks or even months, depending on the severity of destruction and the site's fitness for restoration. As soon as the facility, whether repaired or replaced, is able to support its normal operations, the services may be moved back. The execution team should continue to be engaged until the restoration and testing are complete.

In this phase the original system is restored and execution phase procedures are stopped.

The following major activities occur in this phase

- Continuously monitor the site or facility's fitness for reoccupation
- Verify that the site is free from aftereffects of the disaster and that there are no further threats
- Ensure that all needed infrastructure services, such as power, water, telecommunications, security, environmental controls, office equipment, and supplies, are operational
- Install system hardware, software, and firmware
- Establish connectivity between internal and external systems
- Test system operations to ensure full functionality
- Shut down the contingency system
- Terminate contingency operations
- Secure, remove, and relocate all sensitive materials at the contingency site
- Arrange for operations staff to return to the original facility.

L.O1.3 - Produce a Disaster Recovery Plan Document

- Content/topic 1 : Description of Document Contents

Document Content Text matter of a **document** or publication in any form. **Content** is both information and communication: the sum total of the freshness, readability, relevancy, and usefulness of the information presented, and the manner in which it is presented.

The disaster recovery plan document is the only reliable source of information for the disaster recovery during an emergency. It should be very easily readable, with simple and detailed instructions.

The followings are some of the contents that need to be in this document.

1. **Document Information**

The document should include information such as the authors/owners with their contact details, revision history and other document details (name, location, version), references, and the audience of the document. In the document revision history, it is good to have a brief description of the changes made in each version. A table of contents is a must for quick reference, and it is highly recommended that the sections be numbered to the lowest possible level for easy reference purpose. It is also good to give an appropriate confidential status for the document as it contains sensitive information.

2. **Purpose**

The purpose of the document must be clearly stated in the introduction, defining the objectives the plan intends to achieve.

3. **Scope**

The scope of the plan defines the circumstances under which the plan is invoked and the length of time the procedures defined in the document are in effect. The different failure conditions that lead to invoking the plan should be clearly listed. For example, a system being down for couple of hours may not result in invoking the plan, but a daylong outage may suffice. Similarly, the conditions at the failed system/facility that warrant the reconstitution phase should also be clearly stated.

4. **Assumptions**

Any conditions the plan assumes to be present for success should be clearly stated. This may involve listing the dependencies of the plan as well. For example, a certain number of trained personnel may be assumed to be available at the disaster recovery facility. Wherever possible, these dependencies must be accompanied with the appropriate contact details.

5. **Exclusions**

Any related disaster activities that the plan does not cover should be stated and any known references mentioned here. For example, the plan may exclude the dependent power restoration plan, preferring instead to the appropriate document and the department contact details. Such information will be useful during the disaster recovery.

6. **System Description**

The description of the disaster recovery system should be simple to understand with appropriate figures, workflow charts, and so on. If necessary, the descriptions may reference appendices that give more detail. The functions that need to be revived need to be clearly mentioned.

7. Roles and Responsibilities

The roles of the managerial and technical staff and their responsibilities during the activation, execution, and reconstitution phases should be clearly listed. An organization structure diagram showing the reporting relationships is beneficial. Key roles should have primary and alternate personnel assigned.

8. Contact Details

Full contact information should be included for all the managerial and technical staff involved in the planning, activation, execution, and reconstitution phases. Contact details both during normal situations and emergency situations should be mentioned. This information is recommended to be added as an appendix to the disaster recovery plan document.

9. Activation Procedures

These are procedures for notification, damage assessment, and activation planning should be outlined. Any topic that needs to be covered in great detail may be added as an appendix.

10. Execution Procedures

The recovery procedure for each of the components the plan covers should be explained step by step in detail. When there are parallel threads of tasks, it is beneficial to have a flow chart diagram to visualize the dependencies of the tasks. The success and failure criteria of each procedure also should be mentioned as well as instructions on further actions in case of both success and failure.

11. Reconstitution Procedures

Similar procedures for the reconstitution of the components should be explained in detail. The success and failure criteria and instructions for further actions in case of success and failure should be given.

- Content/Topic 2 : Description of document Maintenance

A **document maintenance** is a formalized system of ensuring that all controlled documents are to the latest configuration or version.

The **disaster recovery plan document** must be kept up to date with the current organization environment. A plan that is not updated and tested is as bad as not having a plan at all because during emergencies, the document may be misleading.

The following are recommended for maintenance of the plan documentation:

1. **Periodic Mock Drills**

The disaster recovery plan should be tested from time to time using scheduled mock drills. A drill usually will not affect active operations; however, if it is known that operations will be affected, the drill should be carefully scheduled such that the effect is minimal and is done during a permissible window. These activities should be regarded similarly to regular equipment maintenance activities that require operations downtime. The experience of the mock drill should be updated into the disaster recovery plan document.

2. **Experience Capture**

The best testing the document will undergo is when an actual disaster happens, and the lessons learned during the disaster recovery are valuable for improving the plan. Hence the Disaster Recovery Committee should ensure that the experience gets captured as lessons learned and the document gets updated accordingly.

3. **Periodic Updates**

Technologies, systems, and facilities that the plan covers may change over time. It is important that the disaster recovery plan document reflect the current information about the components it covers. For this purpose, the Disaster Recovery Committee should ensure that the document is audited periodically (say once every quarter) against the present components in the organization. Another way to achieve this is to ensure that the committee is notified of any change that happens to any system/component in the organization so that the committee may update the document accordingly.

Learning Unit 2 - Implement the written IT disaster Recovery

LO 2.1 - Describe Sequence of backup activities

- Content/Topic 1: Description of Backup software

Backup software is computer programs that perform backup; they create supplementary exact copies of files, databases or entire computers. These programs may later use the supplementary copies to restore the original contents in the event of data loss

Backup software are computer programs which automatically create copies of the information on a computer system so that it can be stored separately and used to replace the original information if it is damaged or lost

A. Key features for backup software.

- **Volume**

  Voluming allows the ability to compress and split backup data into separate parts for storage on smaller so that it will be easier to organize and manage the data that is being stored and backed up.

- **Data compression**

  The process of reducing the size of a data file Compression can be either lossy or lossless.

  Lossless compression reduces bits by identifying and eliminating statistical redundancy. No information is lost in lossless compression.

  Loss compression reduces bits by removing unnecessary or less important information.

  Compressing the data will reduce the size allowing for less drive space to be used to save money.

- **Access to files**

  Many backup solutions offer a plug-in for access to exclusive, in use, and locked files.

- **Schedules**

  Backup schedules are usually supported to reduce maintenance of the backup tool and increase the reliability of the backups.

- **Encryption**

  The process of converting information or data into a code, especially to prevent unauthorized access

  Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users.

  To prevent data theft, some backup software offers cryptography features to protect the backup.

- **Transaction mechanism:** is a fundamental unit of interaction between client and server processes, which encapsulates a sequence of operations to satisfy the properties of ***atomicity*** **(**fact of being composed of indivisible units), ***consistency*** (stability), ***isolation*** **(**apart from others) and ***durability***

(ACID). Transactions that complete successfully are said to ***commit***, those that fail (and appear not to have happened at all) are said to ***abort***.

B. Benefits of backup software.

1. **Schedule backup:** Most software solutions of this kind give users the option to schedule a backup whenever they see fit. This means users don't have to open the software every month to update their stored backup. By scheduling backup, clients are assured that their data is always up-to-date.
2. **Automate the process:** an automated system ready to keep data backed up and restore them at any time will mean less work for the IT department. And of course, business owners are going to enjoy not having to worry about their data as the software will do that job for them.

C. Issues with backup software

1. **Backing up can take a long time:** Depending on how much clients need to backup, this process can consume a lot of time. During the process of backing up files, the servers aren't supposed to be tampered with in any way so that the files won't get corrupted. Although there are fast backup software out there, they still take quite a while to do their jobs.
2. **Minor file errors:** If the backup process is abruptly halted or is finished improperly, there's a good chance that the backed up files will be corrupted and unusable. To counter this, users will need to be very meticulous during the backup process.
3. **Security breaches:** Although majority of the backup software providers guarantee a secure server, there are still cases when cyberattacks get to the backup files.

D. Backup software tools

There are a number of paid-for back software solutions available, but even better is that there are also free versions available so you can discover for yourself which software fits best for you.

The following are the examples of Backup software tools:

- Acronis True Image
- Argentum Backup
- Cloud Berry Backup
- Double Image Backup
- HD Clone
- Total Recovery Pro
- Windows Backup and Restore
- Ease US To do Backup
- Cobia Backup
- Paragon Backup & Recovery
- Ease US to do Backup
- AOMEI Backup per Standard
- Cobia Backup
- File Fort Backup
- Back Up Maker
- Drive Image XML

- COMODO Backup
- Redo Backup
- Yandi’s! Backup
- Everyday Auto Backup
- Mini Tool Shadow Maker
- Imperious Backup
- Genie Timeline Free
- Disk2vhd
- GFI Backup
- Free Ease’s Drive Cloning
- Oster Backup Freeware
- Ace Backup
- F Backup
- HD Clone Free Edition
- Marcum Reflect
- ODIN
- Free byte Backup
- Clone Zillah Live
- Karen's Replicator
- Personal Backup
- Paragon Backup & Recovery Free
- XXCLONE
- PING
- Areca Backup
- Copy Wipe
- G4U

- Content/Topic 2: Description of Common Back-up solution

Definition of Back-up Solution: Back-up Solution is all devices used to store the data or information for avoiding the loss of data.

Capacity, reliability, extensibility, speed, and cost are the issues of driving your backup plan. If you understand how these issues affect your organization, you'll be on track to select an appropriate backup solution.

The most commonly used backup solutions

1. **Tape drives** Tape drives are the most common backup devices. Tape drives use magnetic tape cartridges to store data. Magnetic tapes are relatively inexpensive but aren't highly reliable. Tapes can break or stretch. They can also lose information over time. The average capacity of tape cartridges ranges from 100 MB to 2 GB. Compared with other backup solutions, tape drives are fairly slow. Still, the selling point is the low cost.

2. **Digital audio tapes (DAT)**: tapes DAT drives are quickly replacing standard tape drives as the preferred backup devices. DAT drives use 4 mm and 8 mm tapes to store data. DAT drives and tapes are more expensive than standard tape drives and tapes, but they offer more speed and capacity. DAT drives that use 4 mm tapes can typically record over 30 MB per minute and have capacities of up to 16 GB. DAT drives that use 8 mm tapes can typically record more than 10 MB per minute and have capacities of up to 36 GB (with compression).
3. **Auto-loader tape systems**: Auto-loader tape systems use a magazine of tapes to create extended backup volumes capable of meeting the high-capacity needs of the enterprise. With an auto-loader system, tapes within the magazine are automatically changed as needed during the backup or recovery process. Most auto-loader tape systems use DAT tapes. The typical system uses magazines with between 4 and 12 tapes. The main drawback to these systems is the high cost.

4. **Magnetic optical drives:** Magnetic optical drives combine magnetic tape technology with optical lasers to create a more reliable backup solution than DAT. Magnetic optical drives use 3.5-inch and 5.25-inch disks that look similar to floppies but are much thicker. Typically, magnetic optical disks have capacities of between 1 GB and 4 GB.

5. **Tape Jukeboxes**: Tape jukeboxes are similar to auto-loader tape systems. Jukeboxes use magnetic optical disks rather than DAT tapes to offer high-capacity solutions. These systems load and unload disks stored internally for backup and recovery operations. Their key drawback is the high cost.
6. **Removable disks**: Removable disks, such as Iomega Jaz, are increasingly being used as backup devices. Removable disks offer good speed and ease of use for a single drive or single system backup. However, the disk drives and the removable disks tend to be more expensive than standard tape or DAT drive solutions.
7. **Disk drives Disk**: drives provide the fastest way to back up and restore files. With disk drives, you can often accomplish in minutes what takes a tape drive hour. So when business needs mandate a speedy recovery, nothing beats a disk drive. The drawbacks to disk drives, however, are relatively high costs and less extensibility.

A. **Backup Activities:** The backup activity allows you to create a personalized plan for the content, storage device and schedule of your choice. The backup functionality is available on the Windows version of Toolkit.

LO2.2 - Apply common backup solutions

- Content/Topic 1: Application of Common Back-up solution

A. INTRODUCTION

Losing data because of a computer problem or a hard disk crash is discouraging, to say the least. You might lose family photos, your music collection, or financial data. And, after you get the computer just the way that you want it, it can take a long time to reconfigure your personal settings on a new computer: desktop background, sounds, screensavers, and wireless network configurations to name just a few

However, a little prevention can go a long way to avoiding this ordeal. To help save you lots of time and aggravation, we recommend that you take the precaution of regularly backing up your data and settings.

This article describes how to manually back up your personal files and settings in Windows 7, Windows Vista, Windows XP, and Windows Server 2003. It also describes how to use the data tools in Windows to back up your files and settings.

Method 1: Manually back up your files and settings to removable media or to a network location

The simplest method is to manually back up your files and settings to removable media or a network location. You can specify the files and settings that you want to back up and how often you want to perform a backup.

Note Examples of removable media include external hard disks, DVDs, CDs, and USB memory cards. You can back up files to a different computer or a network device if your computer is connected to a network such as a wireless network.

To manually copy your files to a network location or to removable media on a computer that is running Windows 7, Windows Vista, Windows XP, or Windows Server 2003, follow these steps:

1. Click **Start**

   , click **Computer** and then double-click the drive where you currently have Windows 7, Windows Vista, Windows XP, or Windows Server 2003 installed.
2. Open the Users folder, and then open the user folder that contains the files that you want to back up.
3. Copy the necessary folders from the user folder to a network location or to removable media.

Notes

- To back up data for all users, repeat steps 2–3.
- To determine the size of all the files in the user folder, select all the folders, right-click those selected folders, and then click Properties.
- The saved files can be copied to any computer. However, you must have corresponding applications installed on that computer to open those individual files.
- Not all applications save their files to the user folder. You should make sure that you check other applications and the file system location where the applications save files by default, and then copy those files to the network location or to the removable media.

Method 2: Use the Easy Transfer feature to back up data to a different computer

The next easiest method is to use the Easy Transfer feature in Windows to transfer data to a different computer. This section discusses the following scenarios in which you can use the Easy Transfer feature to back up data to a different computer:

Your computer OS	Target computer OS
Windows 7	Windows 7
Windows 7	Windows Vista
Windows Vista	Windows Vista

Back up a Windows 7-based computer

Transfer files and settings to another Windows 7-based computer

The Windows Easy Transfer feature lets you to back up user account files and settings. Then you can restore those files and settings to a new computer. To start Windows Easy Transfer, follow these steps:

1. Click **Start**, type windows easy transfer in the **Start Search** box, and then click **Windows Easy Transfer** in the **Programs** list.
2. Follow the instructions to transfer your files and settings.

Transfer files and settings to a Windows Vista-based computer

If you want to move your data from a Windows 7-based computer to a Windows Vista-based computer, use the Windows Vista version of Windows Easy Transfer. To do this, follow these steps:

1. On a Windows 7-based computer, insert the Windows Vista CD or DVD
2. Click to exit the Windows Vista Setup program.
3. Click **Start**, click **Computer**, right-click the CD or DVD drive, and then click **Open**.
4. Open the **support** folder, and then open the **migwiz** folder
5. Double-click the Migwiz.exe file.
6. Follow the instructions to begin the transfer from Windows 7.

Back up a Windows Vista-based computer

Transfer files and settings to another Windows Vista-based computer

The Windows Easy Transfer feature lets you to back up user account files and settings. Then you can restore those files and settings to the new computer. To start Windows Easy Transfer, follow these steps:

1. Click **Start**, type transfer in the **Start Search** box, and then click **Windows Easy Transfer** in the **Programs** list.
2. Click **Next**. If you are prompted to close programs, make sure that you have saved any open documents, and then click **Close all**.
3. Follow the steps to transfer files and settings.

Method 3: Use the Backup and Restore Center

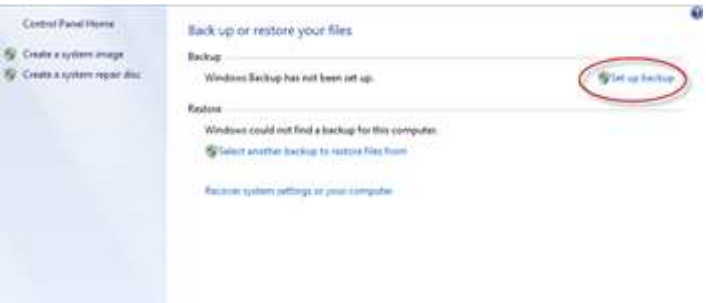
As a precaution, you can use the Backup and Restore Center feature in Windows 7 and Windows Vista to back up your data.

Back up a Windows 7-based computer

Note Data that you back up by using the Windows 7 Backup and Restore Center can be restored only on a Windows 7-based operating system.

1. Click **Start**, type backup in the **Start Search** box, and then click **Backup and Restore** in the **Programs** list.

   Note If you are prompted to close programs, make sure that you have saved any open documents and close those programs. Or, click **Close Programs**.
2. Under **Back up or restore your files**, click **Set up backup**.


Control Panel Home
Create a system image
Create a system repair disc
Set up backup
Select another backup to restore files from
Recover system settings or your computer

Back up or restore your files

Backup

Windows Backup has not been set up.

Restore

Windows could not find a backup for this computer.

3. Select where you want to save your backup, and then click **Next**.

   Note Remember to save your backup files to removable media or a network location.
4. Click **Let Windows choose** or **Let me choose**, and then click **Next**.
5. Make the appropriate selections, and then click **Next** or **Save Settings and run backup**.
6. The backup will be saved to the backup location.

Back up a Windows Vista-based computer

Note Data that you back up by using Windows Vista Backup and Restore Center can be restored only on a Windows Vista operating system.

1. Click **Start**, type backup in the **Start Search** box, and then click **Backup and Restore** in the **Programs** list.
2. Click **Back up files** under **Back up files or your entire computer**.
3. Select where you want to store the file backup, and then click **Next**.
4. Select the disk or disks that you want to back up, and then click **Next**
5. Select the file type or file types that you want to back up, and then click **Next**.
6. Click **Save Settings**, and then start the backup.
7. Your backup will be saved to the selected backup location.

Method 4: Transfer files from a Windows 2000, Windows XP, or Windows Server 2003-based computer

Use the Windows XP Files and Settings Transfer Wizard

You can use the Windows XP Files and Settings Transfer Wizard to transfer files in Windows XP, or Windows Server 2003, or Windows 2000 computer.

1. Click **Start**, click **All Programs**, click **Accessories**, click **System Tools**, and then click **Files and Settings Transfer Wizard**.
2. Click **Next**, click **Old computer**, and then click **Next**.
3. Select how you want to transfer your files. If you select **Other**, you can save to a network location or to removable media so that you can keep a backup for your records.
4. Select what you want to back up, and then click **Next**.

Additional resources

We recommend the following when you back up data:

- Don’t back up your files to a recovery partition or to the same hard disk on which Windows is installed.

Note Manufacturers frequently configure a recovery partition on a computer. Typically, a recovery partition is displayed as a hard disk drive.

- Always store the media that you use for backups in a secure location to prevent unauthorized access to your files.
- Try to use a fireproof location that's separate from your computer's location. Also, consider encrypting the backup data.

Commonly used backup solutions

- Tape drives
- Digital audio tapes (DAT) tapes
- Auto-loader tape systems
- Magnetic optical drives
- Tape Jukeboxes
- Removable disks
- Disk drives

LO2.3 - Perform sequence of recovery activities

- Content/Topic 1: Performing a sequence of recovery activities.

A. Recovery procedures

Recovery procedure is a process that attempts to bring a system back to a normal operating state.

1. Get authorization to access damaged premises or geographic area
2. Notify users associated with the system
3. Obtain required office supplies and work space
4. Obtain and install required hardware components
5. Obtain and load backup media
6. Restore critical operating systems and application software
7. Restore system data
8. Test system functionality including security controls
9. Connect system to network or other external systems

B. Reconstitution Phase

The **reconstitution phase** is when operations return to normal. This occurs when the damage at the affected area has been repaired.

1. Continuously monitor the site or facility’s fitness for reoccupation
2. Verify that the site is free from after effects of the disaster and that there are no further threats
3. Ensure that all needed infrastructure services, such as power, water, telecommunications, Security, environmental controls, office equipment, and supplies, are operational

4. Install system hardware, software, and firmware
5. Establish connectivity between internal and external systems
6. Test system operations to ensure full functionality
7. Shut down the contingency system
8. Terminate contingency operations
9. Secure, remove, and relocate all sensitive materials at the contingency site
10. Arrange for operations staff to return to the original facility

Learning Unit 3 - Document the Work Done

LO3.1 - Document on network status

- Content/Topic 1: Description of the previous network status

B. Network infrastructure

Network infrastructure is the hardware and software resources of an entire network that enable network connectivity, communication, operations and management of an enterprise network. It provides the communication path and services between users, processes, applications, services and external networks/the internet.

1. **Networking Hardware:**
   - Routers
   - Switches
   - LAN cards
   - Wireless routers
   - Cables
2. **Networking Software:**
   - Network operations and management
   - Operating systems
   - Firewall
   - Network security applications
3. **Network Services:**
   - T-1 Line
   - DSL
   - Satellite
   - Wireless protocols
   - IP addressing

C. User manual and previous report

The User Manual contains all essential information for the user to make full use of the information system. This manual includes a description of the system functions and capabilities, contingencies and alternate modes of operation, and step-by-step procedures for system access and use. Use graphics where possible. The manual format may be altered if another format is more suitable for the particular project.

- Content/Topic 2: Identification of the problems

A. Preliminary development

There are several problems in data backup and recovery includes:

1. Corrupted backup
2. Inaccessible backup.
3. Backup job failed to start.
4. Backup job failed to complete
5. Incomplete backup
6. Slow backup

B. Development

Your **disaster recovery plan** depends on backups, so it's important to make sure your backup process works. Don't let these backup problems cause your disaster recovery strategy to fail:

- **Corrupted backup.**

Backups can be corrupt for several reasons. Old media can get damaged or corrupted through poor handling or simply through age. Readable backups may not have application-consistent data, so even though you restore files, applications may not come up successfully.

Solution:

Make multiple copies of backups, preferably on different types of media. Use application-aware backup strategies to ensure you have consistent data.

- **Inaccessible backup.**

If you have only one copy of your backup, and you can't access it during a disaster, you can't use it to restore your data.

Solution:

Make multiple copies of your backup, and store them in at least two different locations.

- **Backup job failed to start.**

If the job doesn't run, the backup isn't created, simple as that.

Solution:

Schedule backup jobs to run automatically, rather than relying on a staffer to manually kick off the job. Automation also eliminates the chance of making errors in parameter settings when starting the job manually.

- **Backup job failed to complete.**

If the job runs into problems during its run, critical data isn't protected.

Solution:

Implement monitoring to alert staff if backup jobs don’t complete successfully. Review your storage capacity frequently to make sure you have enough space for the backup files. Keep track of database growth to make sure you have enough storage space for backups.

- **Incomplete backup.**

Not all incomplete backups are because the job failed to run to completion. Backup procedures may miss files, either because someone thought they weren’t needed or because they never got added to the script.

Solution:

Be comprehensive rather than selective when deciding what to backup. When a new application or database is deployed, make adding it to the backup process part of your change management and deployment process.

- **Slow backup.**

Backup jobs need to complete as part of your end of day process. Slow backup procedures can cause delays that impact the start of work the next day.

Solution:

For backups over the network, make sure you have a reliable network connection with sufficient bandwidth. Keep an eye on database growth and how long backups take to complete; you may need to reschedule the job or do incremental backups in order for the job to complete, with a full backup deferred to weekends or other longer periods of downtime.

C. References

Reference: is the last page of an essay or research paper that's been written in APA style. It lists all the sources you've used in your **project** so readers can easily find what you've cited.

The problems that can be faced in reference are:

1. Lack of informational source
2. No related information

LO3.2 - Report on the work done

- Content/Topic 1: Description of solution implementation

A. Description of procedures of the task accomplished.

A complete backup process should include the following steps:

1. Create a backup of your current databases and any customizations or files specific to your organization’s needs, such as import templates, custom reports, spreadsheets, etc.
2. Store multiple copies of all backup files on external media, such as a tape drive or CD/DVD.
3. **Regularly test your backup**:
    - **Make a backup** of your database
    - Restore from a backup copy. Note: If you're testing a backup for the first time, we recommend restoring the backup in a test environment first (e.g. on a standalone workstation or isolated server). This way, if the backup is bad, restoring to it won't not affect your live database.
    - Verify users can log into the database and that the correct data is present
    - Restore the original data

B. Description of materials used.

1. USB stick

Small, cheap and convenient, USB sticks are everywhere, and their portability means that they’re easy to store safely, but also pretty easy to lose. There are questions about the number of read/write cycles they can take, so should be considered alongside other backup methods.

Advantages (Pros):

- Extremely portable
- Very cheap
- Can easily transfer data to other sources

Disadvantages (Cons):

- Portability means they’re small and easy to lose
- Questions over read/write cycle longevity

1. **External hard drive**

External hard drives are just what they sound like – hard drives that live outside your computer, meaning they can be plugged in to other sources. If using them for backup, it's best not to use them as an 'extra every day hard drive'.

Advantages (Pros):

- Relatively cheap
- Plenty of storage space for larger files

Disadvantages (Cons):

- Potentially open to problems which lost files in the first place (a power surge or malware)

2. **Time Machine**

For the Mac users out there, Time Machine is an option that backs up to external hard drives automatically. Apple sells its own brand of dedicated wireless Time Capsules, but you can use any hard disk for it. Using this method, you'll automatically keep backups hourly for the last 24 hours, daily for the last month and then weekly backups until the machine is full.

Advantages (Pros):

- Automated, meaning you shouldn't forget to stay up to date
- Frequency of backups means you should never be too out of date
- Backs up whole drive, not just the key files

Disadvantages (Cons):

- Dedicated wireless machine is expensive
- Mac only

3. **Network Attached Storage**

Businesses tend to back up their files to network attached storage, but with more and more homes having multiple computers, the idea has a certain appeal, especially for those looking to save files from more than one source. With prices coming down, a dedicated wireless storage solution is a convenient option which requires less thought.

Advantages (Pros):

- Automatic backups mean you don't risk forgetting
- Wireless solutions also work with phones and tablets

Disadvantages (Cons):

- Can be expensive
- Can be awkward to set up and maintain

4. **Cloud Storage**

While network attached storage is essentially your own Cloud Server, there are plenty of third party cloud storage options around: free, paid, or free with paid extras. iCloud, Dropbox, Google Drive and OneDrive are big names, but others are available.

Advantages (Pros):

- Can be done automatically
- A certain amount of space is usually free
- Device agnostic

Disadvantages (Cons):

- Requires an internet connection to work
- You can't account for their security breaches
- Companies aren't obliged to keep these services around forever

5. **Printing**

At a first glance, this might sound a facetious inclusion. But while considerably less technically advanced, printing offers you a hard copy of your most important documents that will survive power outages, and are easy to store and access even if your computer is out of action for a few days. Of course it's hard to keep documents up to date this way, and it won't work for video or audio files, but for that novel you'd be devastated to lose, it's certainly worth considering.

Advantages (Pros):

- A backup that won't be affected by hardware outages or tech headaches
- Impossible for hackers to access

Disadvantages (Cons):

- Impossible for certain file types
- Awkward to manage
- Less practical for longer documents
- Not great for the environment

However, you choose to back up your data (and it's smart to consider using more than one solution, at least for your life-or-death files), make sure that you do it. Often people don't think about what were to happen if their valuable files were to be lost, until it’s too late. Don’t make that mistake, and use World Backup Day to make sure your files are all safe and accounted for.

LO3.3 - Write technical journal and recommendation

- Content/Topic 1: Writing technical journal and Recommendation about current network status

A **technical journal** is a document that describes the process, progress, or results of **technical** or scientific research or the state of a **technical** or scientific research problem. It might also include recommendations and conclusions of the research.

A. Description of Network infrastructure

Network infrastructure is the hardware and software resources of an entire network that enable network connectivity, communication, operations and management of an enterprise network. It provides the communication path and services between users, processes, applications, services and external networks/the internet.

B. Recommendations

Recommendations to protect your data files:

1. Create three sets of daily backups, three sets of weekly backups, and three sets of monthly backups. All media types can fail. Multiple backup copies increase your odds of recovering data if another copy fails.
2. Store one backup set in a safe, off-site location, preferably in a fireproof safe. If you evacuate, bring your backup with you.
3. Periodically test the backup files to ensure your backup system is operating properly and that you are familiar with the database restore procedure.
4. Never overwrite the most recent backup copy on a tape, disk, or CD/DVD.
5. Never process an import, purge, global change without having a current backup.
6. Create a backup schedule and keep it at the computer where the backups are performed.
7. Use a separate backup schedule for each software program.
8. Clearly label your backups with the date and type of data they contain.

C. References

1. https://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-453495.html
2. https://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-453495.html
3. https://www.lifewire.com/free-backup-software-tools-2617964
4. Contingency Planning Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology, by Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, and Ray Thomas. NIST Special Publication 800-34; available at:http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf.